REMARKS

Claims 1-13 and 15-42 are pending in the present application. In the above amendments, claims 1, 2, 3, 8, 11, 13, 15, 18 and 22-36 have been amended, and claims 37-42 have been added.

Applicants respectfully respond to this Office Action.

Claim Rejections – 35 USC § 112

Claims 1-13 and 15-36 were rejected under 35 U.S.C. §112, first paragraph, as allegedly failing to comply with the written description requirement.

The rejections of claims 1-13 and 15-36 as allegedly failing to comply with the written description requirement are respectfully traversed. The examiner asserts that the "specification does not describe receiving data over a broadcast channel, concatenating that data with other data and applying a cryptographic function to the concatenation to determine a key . . . ." See, Office Action, page 4, item 10.

The specification describes, "[i]n one embodiment the function d3 defines a cryptographic type function. In an exemplary embodiment, SK, is computed as: SK=SHA(BAK||SKI) . . . ." See, specification, paragraphs [1087] and [1088]. In the claims, the first part comprises the first key, which, for example, corresponds to the BAK, and second part is based on information sent on the broadcast channel, which second part, for example, corresponds to the SKI. As described in paragraphs [1069] and [1071], a portion of the SKI may be predictable (e.g., SKI_A) such as the system time, and another portion may be sent on the broadcast channel (e.g., SKI_B). Applicants assert that the specification describes the claimed subject matter in a way that reasonably conveys to one skilled in the art that the applicants has possession of the claim invention, and therefore, the specification complies with the written description requirement.

Accordingly, the rejections of claims 1-13 and 15-36 as failing to comply with the written description requirement should be withdrawn.

Claim Rejections – 35 USC § 101

Claims 1-13 and 27-30 were rejected under 35 U.S.C. §101 as allegedly not falling within one of the four statutory categories of invention citing In re Bilski, 88 USPQ2d 1385.

The rejections of claims 1-13 and 27-30 as allegedly not falling within one of the four statutory categories of invention are respectfully traversed. On August 24, 2009, a MEMORANDUM was promulgated containing "Interim Examination Instructions For Evaluating Subject Matter Eligibility Under 35 U.S.C. § 101." The Interim Examination Instructions provide guidance pending a final decision from the Supreme Court in Bilski v. Kappos. There are two criteria for determining subject matter eligibility. The claimed invention (1) must be directed to one of the four statutory categories, and (2) must not be wholly directed to subject matter encompassing a judicially recognized exception. Claims 1-13 and 27-30 recite a process, which is one of the four statutory categories. A process claim, to be statutory under § 101, must pass a machine-or-transformation test, which ensures that the process is limited to a particular practical application. "[T]ransformation of electronic data has been found **when the nature of the data** has been changed such that it has a different function or **is suitable for a different use**." See, Interim Examination Instructions, page 6 (emphasis added).

Claim 1 recites, "encrypting the first key with the registration key" and "sending the encrypted first key to the mobile station participating in the transmission . . . ." The encrypted first key is suitable for a different use than the unencrypted first key. Namely, securely sending the encrypted first key to the mobile station participating in the transmission, which security may not be available for the unencrypted first key. Further, the process is tied to a particular machine, which machine is the mobile station participating in the transmission, because the encrypted first key is sent to the mobile station participating in the transmission. Claims 2-10 and 27-28 depend from independent claim 1.

Claim 11 recites, "receiving a registration key specific to a mobile station participating participant in a transmission", "receiving a first key encrypted with the registration key", "decrypting the first key with the registration key", and "determining a second key using a cryptographic function and the first key, for decrypting content on a broadcast channel . . . ." The decrypted first key is suitable for a different use than the encrypted first key. Namely, the decrypted first key is used to determined a second key, which use may not be available using the

encrypted first key. Further, "[a]n article may can be electronic data that represents a physical object or substance." See, Interim Examination Instructions, page 6. In claim 11, the registration key is specific to a mobile station participating in a transmission. Thus, the process is tied to a particular machine which is the mobile station participating in the transmission. Claims 12-14 and 29-30 depend from independent claim 11.

Accordingly, for the reasons given above, Applicants assert that claims 1-14 and 27-30 recite patentable subject matter.

The rejections of claims 22-23 and 33-36 as allegedly being directed to non-statutory subject matter are respectfully traversed. The examiner asserts that the "claims recite systems with 'means', however, the specification describes the various algorithms and steps could be performed using software alone) pre-grant publication, ¶106, ¶108)." See, Office Action, page 5, item 13.

Claim 22 recites "a wireless communication system." The cited portions of the specification fails to describe a "system" that comprises software alone. Further, claim 22, recites, for example, "means for sending the encrypted first key to the mobile station participating in the transmission." Applicants assert that software alone is not capable of accomplishing this element. As described in the cited paragraph [0108], "[t]he steps of a method or algorithm described in connection with the embodiments herein may be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two."

Similarly, claim 23 recites an "infrastructure element, comprising: means for receiving a registration key specific to a mobile station participating in a transmission; . . ." Applicants assert that software alone is not capable of accomplishing this element. As described in the cited paragraph [0108], "[t]he steps of a method or algorithm described in connection with the embodiments herein may be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two."

Further, an element of a claim expressed as a means for performing a specified function "shall be construed to cover the corresponding structure . . . described in the specification . . . ." 35 U.S.C. § 112, ¶6. "The scope of a 'means' limitation is defined as the corresponding structure or material set forth in the written description and equivalents thereof." See, MPEP 2106 V.A. Further, the USPTO may not disregard structure disclosed in the specification that corresponds to

means (or step) plus function language. In re Donaldson Co.,16 F.3d 1189, 29 USPQ2d 1845 (Fed. Cir. 1994) (emphasis added). By asserting that the claims can cover software alone, without any hardware, the Examiner is not following the clear directive in the statute for construing means for claims, namely, that means for claims "shall be construed to cover the corresponding structure . . . described in the specification." Examples of corresponding structure are clearly shown in Figures 3, 4, 5, 6 and 8A-8D, and described throughout the specification.

Also, as explained in the Manual of Patent Examining Procedure (MPEP), "the burden is on the USPTO to set forth a *prima facie* case of unpatentability. Therefore if USPTO personnel determine that it is more likely than not that the claimed subject matter falls outside all of the statutory categories, they must provide an explanation." MPEP 2106, IV. *B*. Applicants assert that the Examiner has not provided an explanation on why the **wireless communication system** of claim 22 is not a tangible **machine**. Similarly, Applicants assert that the Examiner has not provided an explanation on why the **infrastructure element** of claim 23 is not a tangible **machine**. Instead, the examiner directs attention to steps of a method and algorithm, which are not the subject of claims 22 and 23.

Accordingly, the rejections of claims 22 and 23 as directed to non-statutory subject matter should be withdrawn. Similarly, the rejections of dependent claims 33-36 likewise should be withdrawn.

The rejections of claims 24-26 as allegedly being directed to non-statutory subject matter are respectfully traversed. Claim 24 recites a "**digital storage device**, comprising: first set of instructions for . . . ." As explained in the Interim Examination Instructions "a claim to a **non-transitory, tangible computer readable storage medium** per se that possesses structural limitations under the broadest reasonable interpretation standard to qualify as a **manufacture** would be patent-eligible subject matter. **Adding additional claim limitations to the medium, such as executable instructions or stored data**, to such a statutory eligible claim **would not render the medium non-statutory**, so long as the claim as a whole has a real world use and the medium does not cover substantially all practical uses of a judicial exception. **The claim as a whole remains a tangible embodiment and qualifies as a manufacture.**" See, Interim Examination Instructions, page 4 (emphasis added). Similarly, the digital storage device recited in claim 24 is qualifies as a manufacture, and the additional claim limitations to the

"instructions" doe not render the digital storage device as non-statutory. Accordingly, the rejections of claims 24-26 as directed to non-statutory subject matter should be withdrawn.

Claim Rejections – 35 USC § 103(a)

Claims 1-5, 10-11, 13, 15-16 and 18-24 has been rejected under 35 U.S.C. 103(a) as being unpatentable over the Richards patent in view of a publication by IEEE. Claim 6 has been rejected under 35 U.S.C. 103(a) as being unpatentable over the Richards patent in view of the IEEE publication, and further in view of a publication by LinuxGurux. Claims 7-9 have been rejected under 35 U.S.C. 103(a) as being unpatentable over the Richards patent in view of the IEEE publication, and further in view of a publication by Schneier. Claims 12 and 17 have been rejected under 35 U.S.C. 103(a) as being unpatentable over the Richards patent in view of the IEEE publication, and further in view of U.S. Patent No. 6,073,122 to Wool. Claims 25, 27, 29, 31, 33 and 35 have been rejected under 35 U.S.C. 103(a) as being unpatentable over the Richards patent in view of the IEEE publication, and further in view of U.S. Patent No. 6,536,041 to Knudson et al. Claims 26, 28, 30, 32, 34 and 36 have been rejected under 35 U.S.C. 103(a) as being unpatentable over the Richards patent in view of the IEEE publication, and further in view of U.S. Patent No. 5,778,069 to Thomlinson et al.

The rejection of claim 1 as allegedly unpatentable over the Richards patent in view of the IEEE publication is respectfully traversed. Amended claim 1 is directed to a method for secure transmission, that (among other things) comprises: "updating the second key after a second time period has elapsed, wherein the updated second key is determined based on two parts, a first part comprising the updated first key and a second part based on information sent on the broadcast channel, and wherein the first part and the second part are concatenated to generate the second key using a cryptographic function."

The Richards patent fails to disclose updating the second key after a second time period has elapsed, wherein the updated second key is determined based on two parts, a first part comprising the updated first key and a second part based on information sent on the broadcast channel, and wherein the first part and the second part are concatenated to generate the second key using a cryptographic function. The IEEE publication discloses a secret key concatenated with an initialization vector IV, and the resulting seed input to a pseudo-random number

generator (PRNG). The PRNG outputs a key sequence. The secret key is distributed to cooperating stations (STA by an external key management service. "The secret key remains constant while the IV changes periodically." See, page 64, paragraph 3.

The examiner asserts that the PK (program key) disclosed in the Richards patent is "equivalent to the WEP key." See, Office Action, page 7. Applicants respectfully disagree with this assertion. The PK in the Richards patent changes at times 0, 2, 4, 6, 8, 10, etc. See, Figure 23. In contract, the WEP secret key remains constant. Applicants assert that the WEP secret key is equivalent to the user encryption key variable (UEV) of the Richard patent. See, Figure 26, elements 112 and 133. Thus, Applicants respectfully assets that the IEEE publication fails to remedy the disclosure deficiencies of the Richards patent.

For these reasons, the rejection of claim 1 as allegedly unpatentable over the Richards patent in view of the IEEE publication should be withdrawn.

Claims 2-5 and 10 depend on independent claim 1, and for the reasons discussed above with respect to claim 1, the rejections of claims 2-5 likewise should be withdrawn.

Claims 11, 13, 15-16 and 18-24 are method, infrastructure element, wireless communication system, and digital storage device claims defined by language similar to that discussed above with respect to of method claim 1. For the reasons discussed above with respect to claim 1, the rejections of claims 11, 13, 15-16 and 18-24, as allegedly unpatentable over the Richards patent in view of the IEEE publication, should be withdrawn.

The rejection of claim 6 as being unpatentable over the Richards patent in view of the IEEE publication, and further in view of the LinuxGurux publication is respectfully traversed. Applicants assert that the LinuxGurux publication fails to remedy the disclosure deficiencies of the Richards patent and the IEEE publication as described above with respect to claim 1. Accordingly, Applicant respectfully requests the Examiner to withdraw the rejection of claim 6.

The rejections of claims 7-9 as being unpatentable over the Richards patent in view of the IEEE publication, and further in view of the Schneier publication are respectfully traversed. Applicants assert that the Schneier publication fails to remedy the disclosure deficiencies of the Richards patent and the IEEE publication as described above with respect to claim 1. Accordingly, Applicant respectfully requests the Examiner to withdraw the rejections of claims 7-9.

The rejections of claims 12 and 17 as being unpatentable over the Richards patent in view of the IEEE publication, and further in view of the Wool patent are respectfully traversed. Applicants assert that the Wool patent fails to remedy the disclosure deficiencies of the Richards patent and the IEEE publication as described above with respect to claim 1. Accordingly, Applicant respectfully requests the Examiner to withdraw the rejections of claims 12 and 17.

The rejections of claims 25, 27, 29, 31, 33 and 35 as being unpatentable over the Richards patent in view of the IEEE publication, and further in view of the Knudson patent are respectfully traversed. Applicants assert that the Knudson patent fails to remedy the disclosure deficiencies of the Richards patent and the IEEE publication as described above with respect to claim 1. Accordingly, Applicant respectfully requests the Examiner to withdraw the rejections of claims 25, 27, 29, 31, 33 and 35.

The rejections of claims 26, 28, 30, 32, 34 and 36 as being unpatentable over the Richards patent in view of the IEEE publication, and further in view of the Thomlinson patent are respectfully traversed. Applicants assert that the Thomlinson patent fails to remedy the disclosure deficiencies of the Richards patent and the IEEE publication as described above with respect to claim 1. Accordingly, Applicant respectfully requests the Examiner to withdraw the rejections of claims 26, 28, 30, 32, 34 and 36.

New Claims

New claims 37-42 are supported in the specification at paragraph [1069]. "Some portion of SKI may be predictable. For example, a portion of SKI may be derived from the system time during which SKI is valid. This portion, denoted SKI_A, need not be transmitted to the MS 300 as part of the broadcast service." Applicants respectfully assert that new claims 37-42 recite patentable features over the cited prior art and should be allowed.

REQUEST FOR ALLOWANCE

In view of the foregoing, Applicants submit that all pending claims in the application are patentable. Accordingly, reconsideration and allowance of this application are earnestly solicited. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

Respectfully submitted,

Dated: **December 21, 2009**

By: _____
Won Tae C. Kim, Reg. # 40,457
(858) 651 - 6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502